

110TH CONGRESS
2D SESSION

H. R. 4791

IN THE SENATE OF THE UNITED STATES

JUNE 4, 2008

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Federal Agency Data Protection Act”.

4 (b) TABLE OF CONTENTS.—The table of contents of
5 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Purpose.
- Sec. 3. Definitions.
- Sec. 4. Authority of Director of Office of Management and Budget to establish
information security policies and procedures.
- Sec. 5. Responsibilities of Federal agencies for information security.
- Sec. 6. Federal agency data breach notification requirements.
- Sec. 7. Protection of government computers from risks of peer-to-peer file shar-
ing.
- Sec. 8. Annual independent audit.
- Sec. 9. Best practices for privacy impact assessments.
- Sec. 10. Implementation.

6 **SEC. 2. PURPOSE.**

7 The purpose of this Act is to protect personally iden-
8 tifiable information of individuals that is maintained in or
9 transmitted by Federal agency information systems.

10 **SEC. 3. DEFINITIONS.**

11 (a) PERSONALLY IDENTIFIABLE INFORMATION AND
12 MOBILE DIGITAL DEVICE DEFINITIONS.—Section
13 3542(b) of title 44, United States Code, is amended by
14 adding at the end the following new paragraphs:

15 “(4) The term ‘personally identifiable informa-
16 tion’, with respect to an individual, means any infor-
17 mation about the individual maintained by an agen-
18 cy, including information—

1 “(A) about the individual’s education, fi-
2 nances, or medical, criminal, or employment
3 history;

4 “(B) that can be used to distinguish or
5 trace the individual’s identity, including name,
6 social security number, date and place of birth,
7 mother’s maiden name, or biometric records; or

8 “(C) that is otherwise linked or linkable to
9 the individual.

10 “(5) The term ‘mobile digital device’ includes
11 any device that can store or process information
12 electronically and is designed to be used in a manner
13 not limited to a fixed location, including—

14 “(A) processing devices such as laptop
15 computers, communication devices, and other
16 hand-held computing devices; and

17 “(B) storage devices such as portable hard
18 drives, CD-ROMs, DVDs, and other portable
19 electronic media.”.

20 (b) CONFORMING AMENDMENTS.—Section 208 of the
21 E-Government Act of 2002 (Public Law 107–347; 44
22 U.S.C. 3501 note) is amended—

23 (1) in subsection (b)(1)(A)—

1 (A) in clause (i), by striking “information
 2 that is in an identifiable form” and inserting
 3 “personally identifiable information”; and

4 (B) in clause (ii)(II), by striking “informa-
 5 tion in an identifiable form permitting the phys-
 6 ical or online contacting of a specific indi-
 7 vidual” and inserting “personally identifiable
 8 information”;

9 (2) in subsection (b)(2)(B)(i), by striking “in-
 10 formation that is in an identifiable form” and insert-
 11 ing “personally identifiable information”;

12 (3) in subsection (b)(3)(C), by striking “infor-
 13 mation that is in an identifiable form” and inserting
 14 “personally identifiable information”; and

15 (4) in subsection (d), by striking the text and
 16 inserting “In this section, the term ‘personally iden-
 17 tifiable information’ has the meaning given that
 18 term in section 3542(b)(4) of title 44, United States
 19 Code.”.

20 **SEC. 4. AUTHORITY OF DIRECTOR OF OFFICE OF MANAGE-**
 21 **MENT AND BUDGET TO ESTABLISH INFORMA-**
 22 **TION SECURITY POLICIES AND PROCEDURES.**

23 Section 3543(a) of title 44, United States Code, is
 24 amended—

(1) by inserting before the semicolon at the end of paragraph (5) the following: “, including plans and schedules, developed by the agency on the basis of priorities for addressing levels of identified risk, for conducting—

“(A) testing and evaluation, as required under section 3544(b)(5); and

“(B) remedial action, as required under section 3544(b)(6), to address deficiencies identified by such testing and evaluation”; and

(2) by adding at the end the following:

“(9) establishing minimum requirements regarding the protection of personally identifiable information maintained in or transmitted by mobile digital devices, including requirements for the use of technologies that efficiently and effectively render information unusable by unauthorized persons;

“(10) requiring agencies to comply with—

“(A) minimally acceptable system configuration requirements consistent with best practices, including checklists developed under section 8(c) of the Cyber Security Research and Development Act (Public Law 107–305; 116 Stat. 2378) by the Director of the National Institute of Standards and Technology; and

1 “(B) minimally acceptable requirements
2 for periodic testing and evaluation of the imple-
3 mentation of such configuration requirements;

4 “(11) ensuring that agency contracts for (or in-
5 volving or including) the provision of information
6 technology products or services include requirements
7 for contractors to meet minimally acceptable con-
8 figuration requirements, as required under para-
9 graph (10);

10 “(12) ensuring the establishment through regu-
11 lation and guidance of contract requirements to en-
12 sure compliance with this subchapter with regard to
13 providing information security for information and
14 information systems used or operated by a con-
15 tractor of an agency or other organization on behalf
16 of the agency; and”.

17 **SEC. 5. RESPONSIBILITIES OF FEDERAL AGENCIES FOR IN-**
18 **FORMATION SECURITY.**

19 Section 3544(b) of title 44, United States Code, is
20 amended—

21 (1) in paragraph (2)(D)(iii), by striking “as de-
22 termined by the agency” and inserting “as required
23 by the Director under section 3543(a)(10)”;

24 (2) in paragraph (5)—

1 (A) by inserting after “annually” the fol-
2 lowing: “and as approved by the Director”;

3 (B) by striking “and” at the end of sub-
4 paragraph (A);

5 (C) by redesignating subparagraph (B) as
6 subparagraph (D); and

7 (D) by inserting after subparagraph (A)
8 the following:

9 “(B) shall include testing and evaluation of
10 system configuration requirements as required
11 under section 3543(a)(10);

12 “(C) shall include testing of systems oper-
13 ated by a contractor of the agency or other or-
14 ganization on behalf of the agency, which test-
15 ing requirement may be satisfied by inde-
16 pendent testing, evaluation, or audit of such
17 systems; and”;

18 (3) by striking “and” at the end of paragraph
19 (7);

20 (4) by striking the period at the end of para-
21 graph (8) and inserting a semicolon; and

22 (5) by adding at the end the following:

23 “(9) plans and procedures for ensuring the ade-
24 quacy of information security protections for sys-

1 tems maintaining or transmitting personally identifi-
2 able information, including requirements for—

3 “(A) maintaining a current inventory of
4 systems maintaining or transmitting such infor-
5 mation;

6 “(B) implementing information security re-
7 quirements for mobile digital devices maintain-
8 ing or transmitting such information, as re-
9 quired by the Director (including the use of
10 technologies rendering data unusable by unau-
11 thorized persons); and

12 “(C) developing, implementing, and over-
13 seeing remediation plans to address
14 vulnerabilities in information security protec-
15 tions for such information;”.

16 **SEC. 6. FEDERAL AGENCY DATA BREACH NOTIFICATION**
17 **REQUIREMENTS.**

18 (a) AUTHORITY OF DIRECTOR OF OFFICE OF MAN-
19 AGEMENT AND BUDGET TO ESTABLISH DATA BREACH
20 POLICIES.—Section 3543(a) of title 44, United States
21 Code, as amended by section 4, is further amended—

22 (1) by striking “and” at the end of paragraph

23 (7);

24 (2) in paragraph (8)—

1 (A) by striking “and” at the end of sub-
2 paragraph (D);

3 (B) by striking the period and inserting “;
4 and” at the end of subparagraph (E); and

5 (C) by adding at the end the following new
6 subparagraph:

7 “(F) a summary of the breaches of infor-
8 mation security reported by agencies to the Di-
9 rector and the Federal information security in-
10 cident center pursuant to paragraph (13);”; and
11 (3) by adding at the end the following:

12 “(13) establishing policies, procedures, and
13 standards for agencies to follow in the event of a
14 breach of data security involving the disclosure of
15 personally identifiable information, specifically in-
16 cluding—

17 “(A) a requirement for timely notice to be
18 provided to those individuals whose personally
19 identifiable information could be compromised
20 as a result of such breach, except no notice
21 shall be required if the breach does not create
22 a reasonable risk—

23 “(i) of identity theft, fraud, or other
24 unlawful conduct regarding such indi-
25 vidual; or

1 “(ii) of other harm to the individual;

2 “(B) guidance on determining how timely
3 notice is to be provided;

4 “(C) guidance regarding whether addi-
5 tional special actions are necessary and appro-
6 priate, including data breach analysis, fraud
7 resolution services, identify theft insurance, and
8 credit protection or monitoring services; and

9 “(D) a requirement for timely reporting by
10 the agencies of such breaches to the Director
11 and Federal information security center.”.

12 (b) AUTHORITY OF CHIEF INFORMATION OFFICER
13 TO DEVELOP AND MAINTAIN INVENTORIES.—Section
14 3544(a)(3) of title 44, United States Code, is amended—

15 (1) by inserting after “authority to ensure com-
16 pliance with” the following: “and, to the extent de-
17 termined necessary and explicitly authorized by the
18 head of the agency, to enforce”;

19 (2) by striking “and” at the end of subpara-
20 graph (D);

21 (3) by inserting “and” at the end of subpara-
22 graph (E); and

23 (4) by adding at the end the following:

24 “(F) developing and maintaining an inven-
25 tory of all personal computers, laptops, or any

1 other hardware containing personally identifi-
2 able information;”.

3 (c) INCLUSION OF DATA BREACH NOTIFICATION.—
4 Section 3544(b) of title 44, United States Code, as amend-
5 ed by section 5, is further amended by adding at the end
6 the following:

7 “(10) procedures for notifying individuals
8 whose personally identifiable information may have
9 been compromised or accessed following a breach of
10 information security; and

11 “(11) procedures for timely reporting of infor-
12 mation security breaches involving personally identi-
13 fiable information to the Director and the Federal
14 information security incident center.”.

15 (d) AUTHORITY OF AGENCY CHIEF HUMAN CAPITAL
16 OFFICERS TO ASSESS FEDERAL PERSONAL PROPERTY.—
17 Section 1402(a) of title 5, United States Code, is amend-
18 ed—

19 (1) by striking “, and” at the end of paragraph
20 (5) and inserting a semicolon;

21 (2) by striking the period and inserting “; and”
22 at the end of paragraph (6); and

23 (3) by adding at the end the following:

24 “(7) prescribing policies and procedures for exit
25 interviews of employees, including a full accounting

1 of all Federal personal property that was assigned to
2 the employee during the course of employment.”.

3 **SEC. 7. PROTECTION OF GOVERNMENT COMPUTERS FROM**
4 **RISKS OF PEER-TO-PEER FILE SHARING.**

5 (a) PLANS REQUIRED.—As part of the Federal agen-
6 cy responsibilities set forth in sections 3544 and 3545 of
7 title 44, United States Code, the head of each agency shall
8 develop and implement a plan to ensure the security and
9 privacy of information collected or maintained by or on
10 behalf of the agency from the risks posed by certain peer-
11 to-peer file sharing programs.

12 (b) CONTENTS OF PLANS.—Such plans shall set forth
13 appropriate methods, including both technological (such as
14 the use of software and hardware) and nontechnological
15 methods (such as employee policies and user training), to
16 achieve the goal of securing and protecting such informa-
17 tion from the risks posed by peer-to-peer file sharing pro-
18 grams.

19 (c) IMPLEMENTATION OF PLANS.—The head of each
20 agency shall—

21 (1) develop and implement the plan required
22 under this section as expeditiously as possible, but in
23 no event later than six months after the date of the
24 enactment of this Act; and

1 (2) review and revise the plan periodically as
2 necessary.

3 (d) REVIEW OF PLANS.—Not later than 18 months
4 after the date of the enactment of this Act, the Comp-
5 troller General shall—

6 (1) review the adequacy of the agency plans re-
7 quired by this section; and

8 (2) submit to the Committee on Oversight and
9 Government Reform of the House of Representatives
10 and the Committee on Homeland Security and Gov-
11 ernmental Affairs of the Senate a report on the re-
12 sults of the review, together with any recommenda-
13 tions the Comptroller General considers appropriate.

14 (e) DEFINITIONS.—In this section:

15 (1) PEER-TO-PEER FILE SHARING PROGRAM.—

16 The term “peer-to-peer file sharing program” means
17 computer software that allows the computer on
18 which such software is installed (A) to designate
19 files available for transmission to another such com-
20 puter, (B) to transmit files directly to another such
21 computer, and (C) to request the transmission of
22 files from another such computer. The term does not
23 include the use of such software for file sharing be-
24 tween, among, or within Federal, State, or local gov-

1 ernment agencies in order to perform official agency
2 business.

3 (2) AGENCY.—The term “agency” has the
4 meaning provided by section 3502 of title 44, United
5 States Code.

6 **SEC. 8. ANNUAL INDEPENDENT AUDIT.**

7 (a) REQUIREMENT FOR AUDIT INSTEAD OF EVALUA-
8 TION.—Section 3545 of title 44, United States Code, is
9 amended—

10 (1) in the section heading, by striking “**eval-**
11 **uation**” and inserting “**audit**” ; and

12 (2) in paragraphs (1) and (2) of subsection (a),
13 by striking “evaluation” and inserting “audit” both
14 places it appears.

15 (b) ADDITIONAL SPECIFIC REQUIREMENTS FOR AU-
16 DITS.—Section 3545(a) of such title is amended—

17 (1) in paragraph (2)—

18 (A) in subparagraph (A), by striking “sub-
19 set of the agency’s information systems;” and
20 inserting the following: “subset of—

21 “(i) the information systems used or oper-
22 ated by the agency; and

23 “(ii) the information systems used, oper-
24 ated, or supported on behalf of the agency by
25 a contractor of the agency, any subcontractor

1 (at any tier) of such a contractor, or any other
2 entity;”;

3 (B) in subparagraph (B), by striking
4 “and” at the end;

5 (C) in subparagraph (C), by striking the
6 period and inserting “; and”; and

7 (D) by adding at the end the following new
8 subparagraph:

9 “(D) a conclusion whether the agency’s infor-
10 mation security controls are effective, including an
11 identification of any significant deficiencies in such
12 controls.”; and

13 (2) by adding at the end the following new
14 paragraph:

15 “(3) Each audit under this section shall conform to
16 generally accepted government auditing standards.”.

17 (c) CONFORMING AMENDMENTS.—

18 (1) Each of the following provisions of section
19 3545 of title 44, United States Code, is amended by
20 striking “evaluation” and inserting “audit” each
21 place it appears:

22 (A) Subsection (b)(1).

23 (B) Subsection (b)(2).

24 (C) Subsection (c).

25 (D) Subsection (e)(1).

1 (E) Subsection (e)(2).

2 (2) Section 3545(d) of such title is amended to
3 read as follows:

4 “(d) EXISTING AUDITS.—The audit required by this
5 section may be based in whole or in part on an audit relat-
6 ing to programs or practices of the applicable agency.”.

7 (3) Section 3545(f) of such title is amended by
8 striking “evaluators” and inserting “auditors”.

9 (4) Section 3545(g)(1) of such title is amended
10 by striking “evaluations” and inserting “audits”.

11 (5) Section 3545(g)(3) of such title is amended
12 by striking “Evaluations” and inserting “Audits”.

13 (6) Section 3543(a)(8)(A) of such title is
14 amended by striking “evaluations” and inserting
15 “audits”.

16 (7) Section 3544(b)(5)(D) of such title (as re-
17 designated by section 5(2)(C)) is amended by strik-
18 ing “a evaluation” and inserting “an audit”.

19 **SEC. 9. BEST PRACTICES FOR PRIVACY IMPACT ASSESS-**
20 **MENTS.**

21 Section 208(b)(3) of the E-Government Act of 2002
22 (Public Law 107–347; 44 U.S.C. 3501 note) is amend-
23 ed—

24 (1) in subparagraph (B), by striking “and” at
25 the end;

8 Except as otherwise specifically provided in this Act,
9 implementation of this Act and the amendments made by
10 this Act shall begin not later than 90 days after the date
11 of the enactment of this Act.

Attest: LORRAINE C. MILLER,
Clerk.